11.15.00

A

PTO/SB/05 (08-00)
Approved for use through 10/31/2002. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Please type a plus sign (+) inside this box → ⊞

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UTILITY PATENT APPLICATION TRANSMITTAL

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No.	CISCO-3096
First Inventor	Sheth et al.
Title	PPP/L2TP Domain Name...
Express Mail Label No.	EL575422540US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

1. ☐ Fee Transmittal Form (e.g., PTO/SB/17) *(Submit an original and a duplicate for fee processing)*
2. ☐ Applicant claims small entity status. See 37 CFR 1.27.
3. ☒ Specification [*Total Pages* 40] *(preferred arrangement set forth below)*
   - Descriptive title of the invention
   - Cross Reference to Related Applications
   - Statement Regarding Fed sponsored R & D
   - Reference to sequence listing, a table, or a computer program listing appendix
   - Background of the Invention
   - Brief Summary of the Invention
   - Brief Description of the Drawings *(if filed)*
   - Detailed Description
   - Claim(s)
   - Abstract of the Disclosure
4. ☒ Drawing(s) *(35 U.S.C. 113)* [*Total Sheets* 12]
5. Oath or Declaration [*Total Pages* ☐]
   a. ☐ Newly executed (original or copy)
   b. ☐ Copy from a prior application (37 CFR 1.63 (d)) *(for continuation/divisional with Box 17 completed)*
      i. ☐ DELETION OF INVENTOR(S) Signed statement attached deleting inventor(s) named in the prior application, see 37 CFR 1 63(d)(2) and 1.33(b).
6. ☐ Application Data Sheet. See 37 CFR 1.76

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

7. ☐ CD-ROM or CD-R in duplicate, large table or Computer Program (*Appendix*)
8. Nucleotide and/or Amino Acid Sequence Submission *(if applicable, all necessary)*
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ paper
   c. ☐ Statements verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

9. ☐ Assignment Papers (cover sheet & document(s))
10. ☐ 37 CFR 3.73(b) Statement *(when there is an assignee)* ☐ Power of Attorney
11. ☐ English Translation Document *(if applicable)*
12. ☐ Information Disclosure Statement (IDS)/PTO-1449 ☐ Copies of IDS Citations
13. ☐ Preliminary Amendment
14. ☒ Return Receipt Postcard (MPEP 503) *(Should be specifically itemized)*
15. ☐ Certified Copy of Priority Document(s) *(if foreign priority is claimed)*
16. ☐ Other: .....

17. If a CONTINUING APPLICATION, *check appropriate box, and supply the requisite information below and in a preliminary amendment, or in an Application Data Sheet under 37 CFR 1.76:*

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: _____/_____

Prior application information: *Examiner* _____ *Group / Art Unit:* _____

For CONTINUATION OR DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 5b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

18. CORRESPONDENCE ADDRESS

☐ *Customer Number or Bar Code Label* (Insert Customer No. or Attach bar code label here) or ☐ *Correspondence address below*

Name	David B. Ritchie				
Address	D'Alessandro & Ritchie P. O. Box 640640				
City	San Jose	*State*	CA	*Zip Code*	95164
Country	USA	*Telephone*	408-441-1100	*Fax*	408-441-8400

Name (Print/Type)	John P. Schaub	*Registration No. (Attorney/Agent)*	42,125
Signature	John P Schaub	*Date*	11/13/00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICANT:	Sheth et al.
SERIAL NO.:	(not yet assigned)
FILING DATE:	November 13, 2000
TITLE:	PPP/L2TP DOMAIN NAME PREAUTHORIZATION
EXAMINER:	[not yet assigned]
ART UNIT:	[not yet assigned]

CERTIFICATE OF MAILING

"Express Mail" mailing label no.: EL575422540US
Date of Deposit: November 13, 2000
I hereby certify that this paper is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated above and addressed to: Box PATENT APPLICATION, Commissioner for Patents, Washington, DC 20231, on the date printed below.

Name: Diane Morse
Diane Morse

BOX PATENT APPLICATION
COMMISSIONER FOR PATENTS
WASHINGTON, D.C. 20231

TRANSMITTAL LETTER

Enclosed for filing please find the patent application for an invention entitled, "PPP/L2TP DOMAIN NAME PREAUTHORIZATION", filed on behalf of Cisco Technology, Inc., assignee from inventors Purnam Sheth, Aravind Sitaraman, Charles Yager, and Gregory Burns, including Utility Patent Application Transmittal, 25 pages of specification, 14 pages of claims, 12 sheets of drawing figures, and 1 page of Abstract.

The attorney's Docket Number is CISCO-3096.

Please address all communications regarding this application to:

David B. Ritchie
D'Alessandro & Ritchie
P.O. Box 640640
San Jose, CA 95164-0640
Telephone (408) 441-1100

No fee is being paid at this time.

Respectfully submitted,
D'ALESSANDRO & RITCHIE

Dated: November 13, 2000

John P. Schaub
Reg. No. 42,125

D'Alessandro & Ritchie
P.O. Box 640640
San Jose, CA 95164-0640
(408) 441-1100

UNITED STATES PATENT APPLICATION

FOR

PPP/L2TP DOMAIN NAME PREAUTHORIZATION

INVENTORS:

PURNAM SHETH
ARAVIND SITARAMAN
CHARLES YAGER
GREGORY BURNS

ASSIGNED TO:

CISCO TECHNOLOGY, INC.

PREPARED BY:

D'ALESSANDRO & RITCHIE
P.O. BOX 640640
SAN JOSE, CA 95164-0640
TELEPHONE: (408) 441-1100
FAX: (408) 441-8400

SPECIFICATION

TITLE OF INVENTION

PPP/L2TP DOMAIN NAME PREAUTHORIZATION

BACKGROUND OF THE INVENTION

Cross Reference to Related Applications

This application is related to the following:

U.S. Patent Application Serial No. 09/488,394, filed January 20, 2000 in the name of inventors Aravind Sitaramin, Aziz Abdul, Bernard Janes, Dennis Cox, John Joyce, Peter Heitman, Shujin Zhang and Rene Tio, entitled "System and Method for Identifying a Subscriber for Connection to a Communication Network", commonly assigned herewith.

U.S. Patent Application Serial No. 09/488,395, filed January 20, 2000 in the name of inventors Aravind Sitaramin, Dennis Cox, John Joyce and Shujin Zhang, entitled "System and Method for Determining Subscriber Information", commonly assigned herewith.

U.S. Patent Application Serial No. _____, filed November 13, 2000 in the name of inventors Purnam Sheth, Aravind Sitaraman, Charles Yager and Gregory Burns, entitled "PPP Domain Name and L2TP Tunnel Selection Configuration Override", commonly assigned herewith.

Field of the Invention

The present invention relates to the field of data communications. More particularly, the present invention relates to a system and method for restricting the domains that a subscriber can visit when using Point-to-Point Protocol (PPP).

The Background Art

A significant concern of the individual private and public domains making up the Internet or any other system incorporating multiple networks is the ability to ensure that only those subscribers who are authorized to access the individual private and public domains within the comprehensive network have the capability to access such networks. Serious security risks are posed by the possibility of unauthorized users having the know-how and capability to invade the individual private and public domains within the network.

In today's networking environment, many privately owned domain sites exist on the Internet that allow access only to those individuals which have been granted the proper authorization. For example, these may include company owned private domains containing confidential information and, as such, the company may grant access only to those employed by the company, or they may be communities of interest (i.e. "pay-sites") that provide information only to those subscribers which subscribe to the privately owned domain. The subscriber who connects to the Internet, typically by means of an Internet Service Provider (ISP) or Telephone Company (Telco), may also possess the capability to

assume the identity of an authorized user. This capability heightens the potential for security violations.

Additionally, it is becoming increasingly more prevalent for individual computer users to have the capability to remotely access privately owned intra networks. Such Virtual Private Networks (VPNs) allow the user to connect with the private intra network of the company from the user's residence by means of the telephone line or other convenient means. The inception of wireless remote connections have even made it possible for users to connect from almost any imaginable locale. The ability to connect remotely to individual private intra networks, once seen as a luxury, has become so commonplace that many working professionals require such access in order to accomplish their everyday job assignments. In many instances, remote users connect to privately owned intra networks through the same means that individuals connect to the Internet, typically Telcos or ISPs. VPNs are cost-effective because users can connect to the Internet locally and tunnel back to connect to corporate resources. This reduces overhead costs associated with traditional remote access methods.

Figure 1 shows a simplified diagram of a computer user connected to a computer network 10 via a host computer 12 linked to an access point 14 which grants authorization to external networks or domains 16, 18 and 20. The potential for a network security violation is posed by the user having the capability through the access point 14 to reach or "Knock on the door" of home gateways 22, 24 and 26.

Still referring to Fig. 1, the user has access to the computer networks through a workstation or host computer 12. The host computer 12 has the capability to connect with the external networks through an access point 14. An access point 14 is essentially an external location capable of permitting authorized users to access external computer networks. Typically, the access point consists of a series of Network Access Servers (NASs) and other related hardware, software and/or firmware. An access point 14 may also include a modem pool (not shown) maintained by a Telephone Company (Telco) or an Internet Service Provider (ISP) which enables its authorized users or subscribers to obtain external network access through the host computer 12 which has the required dial-up connection capability. Those of ordinary skill in the art will recognize that other types of access methods may be provided by a Telcos or ISP such as frame relay, leased lines, ATM (Asynchronous Transfer Mode), ADSL (Asymmetric Digital Subscriber Line) and the like.

Typically, when the user desires to access a specified domain, such as the first privately owned secured domain site 16, the user runs a network logon application program on the host computer 12 which requires the user to input user identification and authorization information as a means of initiating access to the desired network. This information is then directed to the access point 14 where it is verified to ensure that the host user has the required authorization to permit access to the desired network. Once authorization is granted to the user, a connection is established via the access point 14 with the home gateway 22 of the specified first privately owned secure domain site 16. The connection established may be a tunnel-based connection, such as L2TP (Layer Two

Tunneling Protocol) or L2F (Layer Two Forwarding), or an IP-based (Internet Protocol) connection, such as used with ATM or frame relay. The user of the host computer 12, having established such a connection, has the ongoing capability to access the specified domain until the connection is terminated either at the directive of the user or by error in data transmission. The access point 14 will typically have the capability to connect the user to various other privately owned secured domain sites, such as the second private domain site 18 or the public Internet 20. The user of the host computer 12 may use the PPP protocol to connect through the wholesaler networks to another Home Gateway.

Layer 2 Tunneling Protocol (L2TP) is used in many Virtual Private Networks (VPNs). An L2TP access concentrator (LAC) is a device that the client directly connects to and that tunnels Point-to-Point (PPP) frames to the L2TP network server (LNS). The LAC is the initiator of incoming calls and the receiver of outgoing calls. An L2TP network server (LNS) is the Termination point for an L2TP tunnel and the access point where PPP frames are processed and passed to higher layer protocols. The LNS handles the server side of the L2TP protocol. The LNS terminates calls arriving at any of the LAC's PPP interfaces, including asynchronous, synchronous and ISDN. The LNS is the initiator of outgoing calls and the receiver of incoming calls.

Figure 2 is a block diagram that illustrates an L2TP tunnel and how a user typically connects to a privately owned domain site such as a corporate intranet. Using L2TP tunneling, an L2TP access concentrator (LAC) 100 located at the ISP's point of presence (POP) 105 exchanges PPP messages 110 with remote users 115 and

communicates by way of L2TP requests and responses with the customer's L2TP network server (LNS) 120 to set up tunnels 125. The L2TP protocol passes protocol-level packets through the virtual tunnel 125 between end points of a point-to-point connection. Frames from remote users are accepted by the ISP's POP 105, stripped of any linked framing or transparency bytes, encapsulated in L2TP and forwarded over the appropriate tunnel 125. The customer's home gateway 120 accepts these L2TP frames, strips the L2TP encapsulation, and processes the incoming frames for the appropriate interface.

Turning now to Fig. 3 a block diagram that illustrates the use of AAA servers in an L2TP tunneling network is presented. The selection of the L2TP tunnel 200 at the LAC 205 or NAS is typically determined by an authentication, authorization and accounting (AAA) server 210 based upon the structured username (uscrname@domain) in the PPP authentication packet. The AAA 210 looks up a service profile that matches the domain name string. The service profile includes the IP address of the L2TP network server (LNS) 215 and a password for the tunnel 200. Once tunnels are established, the LAC 205 forwards the subscriber's PPP session to the destination LNS 215 through the L2TP tunnel 200. The ISP or enterprise customer 220 receives new PPP sessions and authenticates the sessions using AAA server 225. Authenticated sessions are established on the LNS 215, while sessions that fail authentication are rejected.

Present methods of establishing a tunnel allow an unauthorized user to reach or "Knock on the door" of another Home Gateway 215, merely by changing the domain name provided in the PPP authentication packet to the domain name of the intended

Home Gateway 215. In this scenario, all users having access to access point 205 would have the potential to reach the privately owned secured domain site. For example, a user having a domain name of xxx@corpA.com may change the domain name in the PPP authentication packet to xxx@corpB.com, allowing the user's PPP session to be forwarded to the corpB LNS through the L2TP tunnel assigned to corpB. Allowing such unauthorized access to a Home Gateway 215 subjects the Home Gateway 215 to potential security risks, including denial of service attacks.

Denial-of-service attacks typically focus on making a service unavailable for normal use, which is often accomplished by exhausting a resource limitation on the network or within an operating system or application. When involving specific network server applications, these attacks can focus on acquiring and keeping open all of the available connections supported by that server, effectively locking out valid users of the server or service. For example, a user intending to exploit present day L2TP systems could flood the network with many PPP sessions targeted to a Home Gateway for which the user is not authorized. Although the LNS authentication process would typically prevent an unauthorized user from access to the corporate intranet, the resources devoted to handling the large number of PPP sessions could adversely affect the services available to authorized users.

The currently available solutions to this problem are very limited and do not offer the level of security protection that most companies operating secured and confidential private intra networks demand. Companies have been able to minimize the risk by

setting up internal access points which effectively cause the user/host to dial-in or connect directly with the private intra network without going through an external ISP or Telco. While this direct-connect service allows some measure of security it does so at the expense of increasing the costs associated with maintaining an internal access point and the additional connection costs related to remote users having to potentially incur long distance telephone service charges.

What is needed is a solution that provides more control over which domains a particular subscriber may connect to using the PPP protocol.

BRIEF DESCRIPTION OF THE INVENTION

A method for controlling subscriber access in a network capable of establishing connections with a plurality of domains includes receiving a communication from a subscriber using a first communication network coupled to at least one other communication network, the communication optionally including a domain identifier associated with a domain on the at least one other communication network, determining whether the subscriber is authorized to access the domain based upon the domain identifier and a list of authorized domains for a virtual circuit used to receive the communication and authorizing subscriber access to the domain when the domain identifier is included in the list. An access server includes a tunnel ID request generator and an authorizer. The tunnel ID request generator generates a tunnel ID request that includes a virtual circuit identifier associated with a virtual circuit used to accept a PPP authentication request. The authorizer grants subscribers domain access based upon a list of authorized domains for the virtual circuit.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of a computer network wherein the host computer has access to multiple domains within the network.

Fig. 2 is a block diagram that illustrates an L2TP tunnel and how a user typically connects to a corporate intranet.

Fig. 3 is a block diagram that illustrates the use of AAA servers in an L2TP tunneling network.

Fig. 4 is a high-level block diagram of a differentiated computer network that has the capability to limit subscriber access to the system to any domain network selected from a list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention.

Fig. 5 is a high-level flow diagram that illustrates a method for limiting subscriber access to any domain network selected from a list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention.

Fig. 6 is a detailed block diagram of a differentiated computer network that has the capability to limit subscriber access to the system to any domain network selected

from a global list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention.

Fig. 7 is a detailed flow diagram that illustrates a method for determining a tunnel ID based on a path ID and a PPP authentication request domain name in accordance with one embodiment of the present invention.

Fig. 8 is a detailed block diagram of a differentiated computer network that has the capability to limit subscriber access to the system to any domain network selected from a global list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention.

Fig. 9 is a detailed flow diagram that illustrates a method for determining a tunnel ID based on a path ID and a PPP authentication request domain name in accordance with one embodiment of the present invention.

Fig. 10 is a detailed block diagram of a differentiated computer network that has the capability to limit subscriber access to the system to any domain network selected from a local list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention.

Fig. 11 is a detailed flow diagram that illustrates a method for determining a tunnel ID based on a path ID and a PPP authentication request domain name in accordance with one embodiment of the present invention.

Fig. 12 is a table that illustrates associating virtual circuit identifiers with authorized domain names in accordance with one embodiment of the present invention.

Fig. 13 is a table that illustrates associating domain names with tunnel identifiers in accordance with one embodiment of the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Those of ordinary skill in the art will realize that the following description of the present invention is illustrative only and not in any way limiting. Other embodiments of the invention will readily suggest themselves to such skilled persons having the benefit of this disclosure.

In accordance with a presently preferred embodiment of the present invention, the components, processes and/or data structures may be implemented using C++ programs running on high performance computers (such as an Enterprise 2000™ server running Sun Solaris™ as its operating system. The Enterprise 2000™ server and Sun Solaris™ operating system are products available from Sun Microsystems, Inc. of Mountain View, California). Different implementations may be used and may include other types of operating systems, computing platforms, computer programs, firmware and/or general purpose machines. In addition, those of ordinary skill in the art will readily recognize that devices of a less general purpose nature, such as hardwired devices, devices relying on FPGA (field programmable gate array) or ASIC (Application Specific Integrated Circuit) technology, or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herein.

The authentication, authorization and accounting (AAA) service performs user authentication, user authorization and user accounting functions. It may be a Cisco ACS™ product such as Cisco Secure™, available from Cisco Systems, Inc. of San Jose,

California, or an equivalent product. In accordance with one embodiment of the present invention, the Remote Authentication Dial-In User Service (RADIUS) protocol is used as the communication protocol for carrying AAA information. RADIUS is an Internet standard track protocol for carrying authentication, authorization, accounting and configuration information between devices that desire to authenticate their links and a shared AAA or AAA proxy service. Those of ordinary skill in the art will realize that other authentication protocols such as TACACS+ or DIAMETER can be used as acceptable authentication communications links between the various communications devices that encompass the data communications network and still be within the inventive concepts disclosed herein.

Turning now to Fig. 4, a block diagram that illustrates a communication system 300 in accordance with one embodiment of the present invention is presented. Users connect to public or private domain networks within communication system 300 through host computers 305, 310, 315. The host computers 305, 310, 315 have the capability to connect or link with domain 320. Domain 320 may be a private domain or a public domain, such as the Internet or a private intra network. These links or connections are established via a series of hardware that serve to grant access to specific domains and transport data packets to and from the host computers 305, 310, 315 and domain 320.

The host computers 305, 310, 315 in this particular computer network are connected to a Publicly Switched Telephone Network (PSTN) 325 via a transmission means 330, 335, 340, such as copper wire or cable. Broadcast mechanisms such as

ADSL (Asymmetric Digital Subscriber Line) may be used. Those of ordinary skill in the art will recognize that other types of broadcast mechanisms may be provided by an ISP or Telco such as Ethernet, frame relay, leased lines, ATM (Asynchronous Transfer Mode) or the like. Access points 345 are located within a wide area network (WAN) 350 and are operated by Telcos or ISPs. The access points 345 house AAA servers 355, Service Selection Gateways (not shown in Fig. 4), L2TP Access Concentrators (LACs) 360, Digital Subscriber Line Aggregation Multiplexers (DSLAMs) 365, 370, 375 or similar devices. The Service Selection Gateway (SSG) is not an integral part of the present invention and therefore a discussion related to their functionality would not benefit the discussion of the present invention. The SSG serves as a gateway between the user and public area domains, such as the Internet. In order for a user host to gain access to a public domain network, such as the Internet, users must first dial-in or otherwise make a connection with the SSG through a data-receiving interface (not shown in Fig. 5.). As a threshold matter, an authorizer (not shown in Fig. 5) within the LAC serves to authenticate the identity of the user, ensure authorization and ascertain the nature and scope of the public network services that it will provide.

According to one embodiment of the present invention, an access point 345 includes one or more DSLAMs 365, 370, 375 that service the copper loops between the access point 345 and the Customer Premises Equipment (CPE) 305, 310, 315. DSLAMs 365, 370, 375 may link locally or via an inter-central office (CO) link to LAC 360. Traffic enters and exits the DSLAM chassis through ports, each of which is assigned a port address. A virtual circuit or channel (VC) is a logical circuit created to ensure

reliable communication between two network devices. A VC is defined by a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI) pair, which is directly tied to a particular DSLAM port used by a particular subscriber.

The LAC 360 is linked to a separate server/memory device 355, herein referred to as an Authentication, Authorization and Accounting (AAA) server 355. The LAC 360 and the AAA server 355 communicate with one-another according to the Remote Access Dial-In User Service (RADIUS) protocol. The specific details of the RADIUS protocol are well known by those of ordinary skill in the art. Moreover, as will be apparent to those of ordinary skill in the art, the RADIUS protocol has limited applicability to the present invention and, therefore a detailed discussion of this protocol is deemed unnecessary. The preferred methods of the present invention described herein are not limited to the use of the RADIUS protocol and other equivalent authentication protocols may be used.

In accordance with one embodiment of the present invention, the LAC service and the LNS may be implemented using a Cisco 6400 Universal Access Concentrator, available from Cisco Systems, Inc. of San Jose, California.

Turning now to Fig. 5, a high-level flow diagram that illustrates a method for limiting subscriber access to any domain network selected from a list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention is presented. At 500, a PPP session authentication request that includes a

domain name is received. At 505, a tunnel ID is determined, based upon the domain name and a virtual circuit identifier such as a VPI/VCD identifier. At 510, a determination is made regarding whether the domain name is authorized. If the domain name is unauthorized, the call is dropped at 515. If the domain is authorized, the PPP session is forwarded onto the tunnel at 520.

Figures 6-11 illustrate three different embodiments of the present invention. Figures 6-7 and 8-9 illustrate two embodiments that maintain domain restriction data globally in an AAA server or similar device. The embodiment illustrated by Figures 6-7 requires two message exchanges between an AAA server and a LAC device, while the embodiment illustrated by Figures 8-9 requires only one message exchange. Figures 10-11 illustrate an embodiment of the present invention that maintains domain restriction data locally in a LAC or similar device.

Turning now to Fig. 6, a detailed block diagram of a differentiated computer network that has the capability to limit subscriber access to the system to any domain network selected from a global list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention is presented. A first receiving interface 600 of LAC 605 receives a PPP authentication request 610. The PPP authentication request 610 includes a domain name 615. The request 610 is received at a particular DSLAM port associated with a virtual circuit identifier such as a VPI/VCI identifier. A domain list request generator 620 generates a domain list request packet and a first forwarding interface 625 sends a request packet to an AAA server 630. The packet

includes the virtual circuit identifier 635 associated with the virtual channel used to receive the PPP session 610. The AAA server 630 receives the domain list request 640, performs a table lookup using table 645 to obtain a list of authorized domain names associated with the virtual circuit ID and returns the list of authorized domain names 650. A second receiving interface 655 receives the list of authorized domain names 650. An assessor 660 determines whether the domain identifier 615 is in the list of authorized domain names 650. If the domain name 615 is not in the list of authorized domain names 650, the call is dropped. If the domain name 615 is in the list of authorized domain names 650, a tunnel ID request generator 660 generates a tunnel ID request and a second forwarding interface 665 sends the tunnel ID request 670 to the AAA server 630. The tunnel ID request 670 includes the PPP authentication packet domain name 615. The AAA server 630 receives the tunnel ID request 670, performs a table lookup using table 675 to obtain the tunnel ID associated with the PPP authentication packet domain name 610 and returns the tunnel ID 680. A third receiving interface 685 receives the tunnel ID 680. An authorizer 690 authorizes user access to the domain 610 when the assessor 660 determines access is authorized and when a tunnel ID 680 is received. A third forwarding interface 690 forwards the PPP session 610 to the LNS 695 associated with the tunnel ID 680.

Turning now to Fig. 7, a detailed flow diagram that illustrates a method for determining a tunnel ID based on a path ID and a PPP authentication request domain name in accordance with one embodiment of the present invention is presented. Figure 7 provides more detail for reference numeral 505 of Fig. 5. At 700, an authorized domain

list request including a virtual circuit ID is sent to an AAA server. At 705, a list of authorized domains for the virtual circuit ID is received. At 710, a determination is made regarding whether the PPP authentication request domain name is in the list of authorized domain names. If the domain name is not in the list, an indication that the domain name is unauthorized is made at 715. If the domain name is in the list, at 720, a tunnel ID request including the PPP authentication request domain name is sent to the AAA server. At 725, a tunnel ID associated with the PPP authentication request domain name is received.

Figures 8 and 9 illustrate another embodiment of the present invention that maintains domain restriction data globally in an AAA server or similar device. The embodiment requires only one message exchange between an LAC device and an AAA server.

Turning now to Fig. 8, a detailed block diagram of a differentiated computer network that has the capability to limit subscriber access to the system to any domain network selected from a global list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention is presented. A first receiving interface 800 of LAC 805 receives a PPP authentication request 810 that includes a domain name 850. The request 810 is received at a particular DSLAM port associated with a virtual circuit identifier 815 such as a VPI/VCI identifier. A tunnel ID request generator 820 generates a tunnel ID request 825 and a first forwarding interface 830 sends the tunnel ID request 825 to the AAA server 835. The tunnel ID request 825

includes the virtual circuit ID 815 associated with the virtual circuit used to receive the PPP authentication request 810 and the domain name included in the PPP authentication request 850. An AAA server 835 receives the tunnel ID request 825 and performs a table lookup using table 840 to obtain a list of authorized domain names associated with the virtual circuit ID. An assessor 845 determines whether the domain name included in the PPP authentication request 850 is in the list of authorized domain names. If the domain name 850 is not in the list of authorized domain names, an indication that the domain access is unauthorized is made. If the domain name 850 is in the list of authorized domain names, the AAA server 835 performs a table lookup using table 855 to obtain the tunnel ID 860 associated with the PPP authentication packet domain name 850. The AAA server 835 returns the authorization indication 865 and the tunnel ID 860. A second receiving interface 870 receives the authorization indication 865 and tunnel ID 860. An authorizer 875 authorizes user access to the domain 850 according to the authorization indication 865. A third forwarding interface 880 forwards the PPP session 810 to the LNS 885 associated with the tunnel ID 860. If domain access is unauthorized, the call is dropped.

Turning now to Fig. 9, a detailed flow diagram that illustrates a method for determining a tunnel ID based on a path ID and a PPP authentication request domain name in accordance with one embodiment of the present invention is presented. Figure 9 provides more detail for reference numeral 505 of Fig. 5. At 900, a tunnel ID request including a virtual circuit identifier such as a VPI/VCI ID and the PPP authentication request domain name are sent to an AAA server. The AAA server determines whether

the subscriber access to the domain is authorized. If subscriber access is authorized, the AAA server determines the tunnel ID associated with the domain. At 905, the tunnel ID and an indication of whether the PPP authentication request domain name is authorized are received from the AAA server.

Figures 10 and 11 illustrate an embodiment of the present invention that maintains domain restriction data locally in a LAC or similar device. Figure 10 is a detailed block diagram of a differentiated computer network that has the capability to limit subscriber access to the system to any domain network selected from a global list of domain networks associated with a virtual circuit in accordance with one embodiment of the present invention. A receiving interface 1000 of LAC 1005 receives a PPP authentication request 1010 that includes a domain name 1015. The PPP authentication request request 1010 is received at a particular DSLAM port associated with a virtual circuit identifier 1020 such as a VPI/VCI identifier. An authorized domain list determiner 1025 performs a table lookup using table 1030 to obtain a list of authorized domain names associated with the virtual circuit ID 1020 associated with the virtual channel used to receive the PPP session 1010. An assessor 1035 determines whether the domain name 1015 included in the PPP authentication request 1010 is in the list of authorized domain names. If the domain name 1015 is not in the list of authorized domain names, the call is dropped. If the domain name 1015 is in the list of authorized domain names, a tunnel ID determiner 1040 performs a table lookup using table 1045 to obtain the tunnel ID associated with the PPP authentication packet domain name 1015. An authorizer 1050 authorizes user access to the domain 1015 when the domain name 1015 is in the list of authorized domain

names. A forwarding interface 1055 forwards the PPP session 1010 to the LNS 1060 associated with the tunnel ID.

Turning now to Fig. 11, a detailed flow diagram that illustrates a method for determining a tunnel ID based on a path ID and a PPP authentication request domain name in accordance with one embodiment of the present invention is presented. Figure 11 provides more detail for reference numeral 505 of Fig. 5. At 1100, a table lookup based on a virtual circuit ID such as a VPI/VCI identifier is performed to obtain a list of authorized domain names associated with the virtual circuit ID. At 1105, a determination is made regarding whether the PPP authentication request domain name is in the list of authorized domain names. If the domain name is not in the list, an indication that the domain name is unauthorized is made at 1110. If the domain name is in the list, at 1115, a table lookup based on the domain name is performed to obtain the tunnel ID associated with the domain name.

Figures 12-13 are tables that illustrate tunnel configuration information that may be stored in a LAC, an AAA server, or other similar devices in accordance with embodiments of the present invention. Figure 12 is a table that illustrates associating virtual circuit identifiers 1200 with authorized domain names 1205 in accordance with one embodiment of the present invention. Figure 13 is a table that illustrates associating domain names 1300 with tunnel identifiers 1305 in accordance with one embodiment of the present invention. In the example, a port having a virtual circuit ID of 10/2 (1210)

may establish tunnels with corpA.com (1215, 1310) or corpB.com (1220, 1315), using tunnel IDs 1320 and 1325, respectively.

According to embodiments of the present invention, the information contained in the tables illustrated in Figs. 12 and 13 is requested by the domain owner to be placed in AAA servers or LACs. It allows the service provider or wholesaler the capability to restrict which domains a PPP session originating from a particular DSLAM port may connect to. This provides added security to the owner of the private domain by lessening the likelihood of an unauthorized access to the home gateway of a corporate intranet. It also allows a wholesaler to charge service providers and subscribers based on which domains are authorized. The service provider or wholesaler would have the control over which ports are allocated to which domains and are, thus, limited to those domains.

Although embodiments of the present invention is have been described with respect to virtual circuits in an ATM networking environment, it should be understood that a virtual circuit assigned to a subscriber in system may be defined in any suitable networking environment using any suitable communication technologies and protocols, without deviating from the scope of the present invention.

In accordance with a specific embodiment of the present invention, the components, process steps, and/or data structures are implemented using software. This implementation is not intended to be limiting in any way. Different implementations may be used and may include other types of operating systems, computing platforms, and/or

computer programs. In addition, those of ordinary skill in the art will readily recognize that devices of a less general purpose nature, such as hardwired devices, devices relying on FPGA (field programmable gate array) or ASIC (application specific integrated circuit) technology, or the like, may also be used without departing from the scope and spirit of the inventive concepts disclosed herewith.

While embodiments and applications of this invention have been shown and described, it would be apparent to those skilled in the art having the benefit of this disclosure that many more modifications than mentioned above are possible without departing from the inventive concepts herein. The invention, therefore, is not to be restricted except in the spirit of the appended claims.

CLAIMS

What is claimed is:

1. A method for controlling subscriber access in a network capable of establishing connections with a plurality of domains, comprising:

receiving a communication from a subscriber using a first communication network coupled to at least one other communication network, said communication optionally including a domain identifier associated with a domain on said at least one other communication network;

determining whether said subscriber is authorized to access said domain based upon said domain identifier and a list of authorized domains for a virtual circuit used to receive said communication;

authorizing subscriber access to said domain when said domain identifier is included in said list.

2. The method of claim 1, further comprising terminating said communication when said domain identifier is not included in said list.

3. The method of claim 1 wherein said communication comprises a Point-to-Point Protocol (PPP) session.

4. The method of claim 3 wherein

said PPP session comprises a tunneling session;

said determining further comprises assigning a tunnel ID; and

said PPP session is forwarded onto a tunnel associated with said tunnel ID when said subscriber is authorized to access said domain.

5. The method of claim 4 wherein said tunneling session comprises an L2TP session.

6. The method of claim 5 wherein said determining further comprises:

issuing an authorized domain list request including a virtual circuit identifier;

receiving an authorized domain list that includes authorized domains for said identifier;

indicating said domain is unauthorized when said domain name is not in said domain list;

indicating said domain is authorized when said domain name is in said domain list;

issuing a tunnel ID request including said domain name when said domain name is authorized; and

receiving a tunnel ID.

7. The method of claim 6 wherein

said authorized domain list request is serviced by an AAA server; and

an AAA server services said tunnel ID request.

8. The method of claim 6 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

9. The method of claim 5 wherein said determining further comprises:

issuing a tunnel ID request including said domain name and a virtual circuit identifier; and

receiving a tunnel ID.

10. The method of claim 9 wherein an AAA server services said tunnel ID request.

11. The method of claim 9 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

12. The method of claim 5 wherein said determining further comprises:

performing a table lookup based on a virtual circuit identifier to obtain an authorized domain list that includes authorized domains for said virtual circuit identifier;

indicating said domain is unauthorized when said domain name is not in said authorized domain list;

indicating said domain is authorized when said domain name is in said authorized domain list; and

performing a table lookup based on said domain name to obtain a tunnel ID when said domain name is authorized.

13. The method of claim 12 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

14. A program storage device readable by a machine, embodying a program of instructions executable by the machine to perform a method to control subscriber

access in a network capable of establishing connections with a plurality of domains, the method comprising:

receiving a communication from a subscriber using a first communication network coupled to at least one other communication network, said communication optionally including a domain identifier associated with a domain on said at least one other communication network;

determining whether said subscriber is authorized to access said domain based upon said domain identifier and a list of authorized domains for a virtual circuit used to receive said communication;

authorizing subscriber access to said domain when said domain identifier is included in said list.

15. The program storage device of claim 14, further comprising terminating said communication when said domain identifier is not included in said list.

16. The program storage device of claim 14 wherein said communication comprises a Point-to-Point Protocol (PPP) session.

17. The program storage device of claim 16 wherein

said PPP session comprises a tunneling session;

said determining further comprises assigning a tunnel ID; and

said PPP session is forwarded onto a tunnel associated with said tunnel ID when said subscriber is authorized to access said domain.

18. The program storage device of claim 17 wherein said tunneling session comprises an L2TP session.

19. The program storage device of claim 18 wherein said determining further comprises:

issuing an authorized domain list request including a virtual circuit identifier;

receiving an authorized domain list that includes authorized domains for said identifier;

indicating said domain is unauthorized when said domain name is not in said domain list;

indicating said domain is authorized when said domain name is in said domain list;

issuing a tunnel ID request including said domain name when said domain name is authorized; and

receiving a tunnel ID.

20. The program storage device of claim 19 wherein

said authorized domain list request is serviced by an AAA server; and

an AAA server services said tunnel ID request.

21. The program storage device of claim 19 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

22. The program storage device of claim 18 wherein said determining further comprises:

issuing a tunnel ID request including said domain name and a virtual circuit identifier; and

receiving a tunnel ID.

23. The program storage device of claim 22 wherein an AAA server services said tunnel ID request.

24. The program storage device of claim 22 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

25. The program storage device of claim 18 wherein said determining further comprises:

performing a table lookup based on a virtual circuit identifier to obtain an authorized domain list that includes authorized domains for said virtual circuit identifier;

indicating said domain is unauthorized when said domain name is not in said authorized domain list;

indicating said domain is authorized when said domain name is in said authorized domain list; and

performing a table lookup based on said domain name to obtain a tunnel ID when said domain name is authorized.

26. The program storage device of claim 25 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

27. An apparatus for controlling subscriber access in a network capable of establishing connections with a plurality of domains, the apparatus comprising:

means for receiving a communication from a subscriber using a first communication network coupled to at least one other communication network, said communication optionally including a domain identifier associated with a domain on said at least one other communication network;

means for determining whether said subscriber is authorized to access said domain based upon said domain identifier and a list of authorized domains for a virtual circuit used to receive said communication;

means for authorizing subscriber access to said domain when said domain identifier is included in said list.

28. The apparatus of claim 27, further comprising means for terminating said communication when said domain identifier is not included in said list.

29. The apparatus of claim 27 wherein said communication comprises a Point-to-Point Protocol (PPP) session.

30. The apparatus of claim 29 wherein

said PPP session comprises a tunneling session;

said determining further comprises means for assigning a tunnel ID; and

said PPP session is forwarded onto a tunnel associated with said tunnel ID when said subscriber is authorized to access said domain.

31. The apparatus of claim 30 wherein said tunneling session comprises an L2TP session.

32. The apparatus of claim 29 wherein said determining further comprises:

means for issuing an authorized domain list request including a virtual circuit identifier;

means for receiving an authorized domain list that includes authorized domains for said identifier;

means for indicating said domain is unauthorized when said domain name is not in said domain list;

means for indicating said domain is authorized when said domain name is in said domain list;

means for issuing a tunnel ID request including said domain name when said domain name is authorized; and

means for receiving a tunnel ID.

33. The apparatus of claim 32 wherein

said authorized domain list request is serviced by an AAA server; and

an AAA server services said tunnel ID request.

34. The apparatus of claim 32 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

35. The apparatus of claim 31 wherein said determining further comprises:

means for issuing a tunnel ID request including said domain name and a virtual circuit identifier; and

means for receiving a tunnel ID.

36. The apparatus of claim 35 wherein an AAA server services said tunnel ID request.

37. The apparatus of claim 35 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

38. The apparatus of claim 31 wherein said determining further comprises:

means for performing a table lookup based on a virtual circuit identifier to obtain an authorized domain list that includes authorized domains for said virtual circuit identifier;

means for indicating said domain is unauthorized when said domain name is not in said authorized domain list;

means for indicating said domain is authorized when said domain name is in said authorized domain list; and

means for performing a table lookup based on said domain name to obtain a tunnel ID when said domain name is authorized.

39. The apparatus of claim 38 wherein said virtual circuit identifier comprises a VPI/VCI identifier.

40. An access server capable of forcing subscribers of a communications system to gain access exclusively to a domain network associated with a virtual circuit, said access server comprising:

an authorized domain list request generator capable of generating an authorized domain list request including a virtual circuit identifier associated with a virtual circuit used to accept a PPP session authentication request, said PPP session authentication request including a domain identifier;

an assessor capable of determining whether said domain identifier is in said domain list;

a tunnel ID request generator capable of generating a tunnel ID request including said domain identifier; and

an authorizer capable of granting users domain access based upon said authorized domain list.

41. The access server of claim 40, further comprising:

a first receiving interface capable of accepting said PPP session authentication request;

a first forwarding interface capable of sending said authorized domain list request to an AAA server;

a second receiving interface capable of accepting a requested authorized domain list;

a second forwarding interface capable of sending said tunnel ID request to an AAA server;

a third receiving interface capable of accepting a requested tunnel ID; and

a third forwarding interface capable of forwarding said PPP session on a tunneling session associated with said tunnel ID.

42. The access server of claim 40 wherein said tunneling session comprises an L2TP session.

43. The access server of claim 42 wherein said virtual circuit identifier comprises a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI).

44. The access server of claim 43 wherein said first receiving interface comprises at least one access multiplexer, each access multiplexer having a plurality of inputs for receiving a service request, each of said inputs being associated with a particular subscriber virtual circuit.

45. The access server of claim 41 wherein said AAA server and said access server communicate using the Remote Authorization Dial-In User Service (RADIUS) protocol.

46. An access server capable of forcing subscribers of a communications system to gain access exclusively to a domain network associated with a virtual circuit, said access server comprising:

a tunnel ID request generator capable of generating a tunnel ID request, said tunnel ID request including a virtual circuit identifier associated with a virtual circuit used to accept a PPP authentication request; and

an authorizer capable of granting users domain access based upon a list of authorized domains for said virtual circuit.

47. The access server of claim 46, further comprising:

a first receiving interface capable of accepting said PPP session authentication request, said PPP session authentication request including a domain identifier;

a first forwarding interface capable of sending said tunnel ID request to an AAA server;

a second receiving interface capable of accepting a requested tunnel ID; and

a second forwarding interface capable of forwarding said PPP session on a tunneling session associated with said tunnel ID.

48. The access server of claim 47 wherein said tunneling session comprises an L2TP session.

49. The access server of claim 48 wherein said virtual circuit identifier comprises a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI).

50. The access server of claim 46 wherein said first receiving interface comprises at least one access multiplexer, each access multiplexer having a plurality of inputs for receiving a service request, each of said inputs being associated with a particular subscriber virtual circuit.

51. The access server of claim 47 wherein said AAA server and said access server communicate using the Remote Authorization Dial-In User Service (RADIUS) protocol.

52. An access server capable of forcing subscribers of a communications system to gain access exclusively to a domain network associated with a virtual circuit, said access server comprising:

a memory device capable of storing a domain list table and a tunnel ID table, said domain list table including a plurality of virtual circuit identifiers and associated

domain identifiers, said tunnel ID table including a plurality of domain names and associated tunnel IDs;

an authorized domain list determiner capable of determining an authorized domain list based upon said domain list table and a domain identifier within a PPP authentication request, said PPP authentication request received on a virtual circuit having a virtual circuit identifier;

an assessor capable of determining whether said domain identifier is in said domain list;

a tunnel ID determiner capable of determining a tunnel ID based upon said tunnel ID table and said domain identifier; and

an authorizer capable of granting subscribers domain access based upon said authorized domain list.

53. The access server of claim 51, further comprising:

a receiving interface capable of accepting said PPP session authentication request; and

a forwarding interface capable of forwarding said PPP session on a tunneling session associated with said tunnel ID.

54. The access server of claim 53 wherein said tunneling session comprises an L2TP session.

55. The access server of claim 54 wherein said virtual circuit identifier comprises a Virtual Path Identifier (VPI) / Virtual Channel Identifier (VCI).

56. The access server of claim 52 wherein said first receiving interface comprises at least one access multiplexer, each access multiplexer having a plurality of inputs for receiving a service request, each of said inputs being associated with a particular subscriber virtual circuit.

ABSTRACT OF THE DISCLOSURE

A method for controlling subscriber access in a network capable of establishing connections with a plurality of domains includes receiving a communication from a subscriber using a first communication network coupled to at least one other communication network, the communication optionally including a domain identifier associated with a domain on the at least one other communication network, determining whether the subscriber is authorized to access the domain based upon the domain identifier and a list of authorized domains for a virtual circuit used to receive the communication and authorizing subscriber access to the domain when the domain identifier is included in the list. An access server includes a tunnel ID request generator and an authorizer. The tunnel ID request generator generates a tunnel ID request that includes a virtual circuit identifier associated with a virtual circuit used to accept a PPP authentication request. The authorizer grants subscribers domain access based upon a list of authorized domains for the virtual circuit.

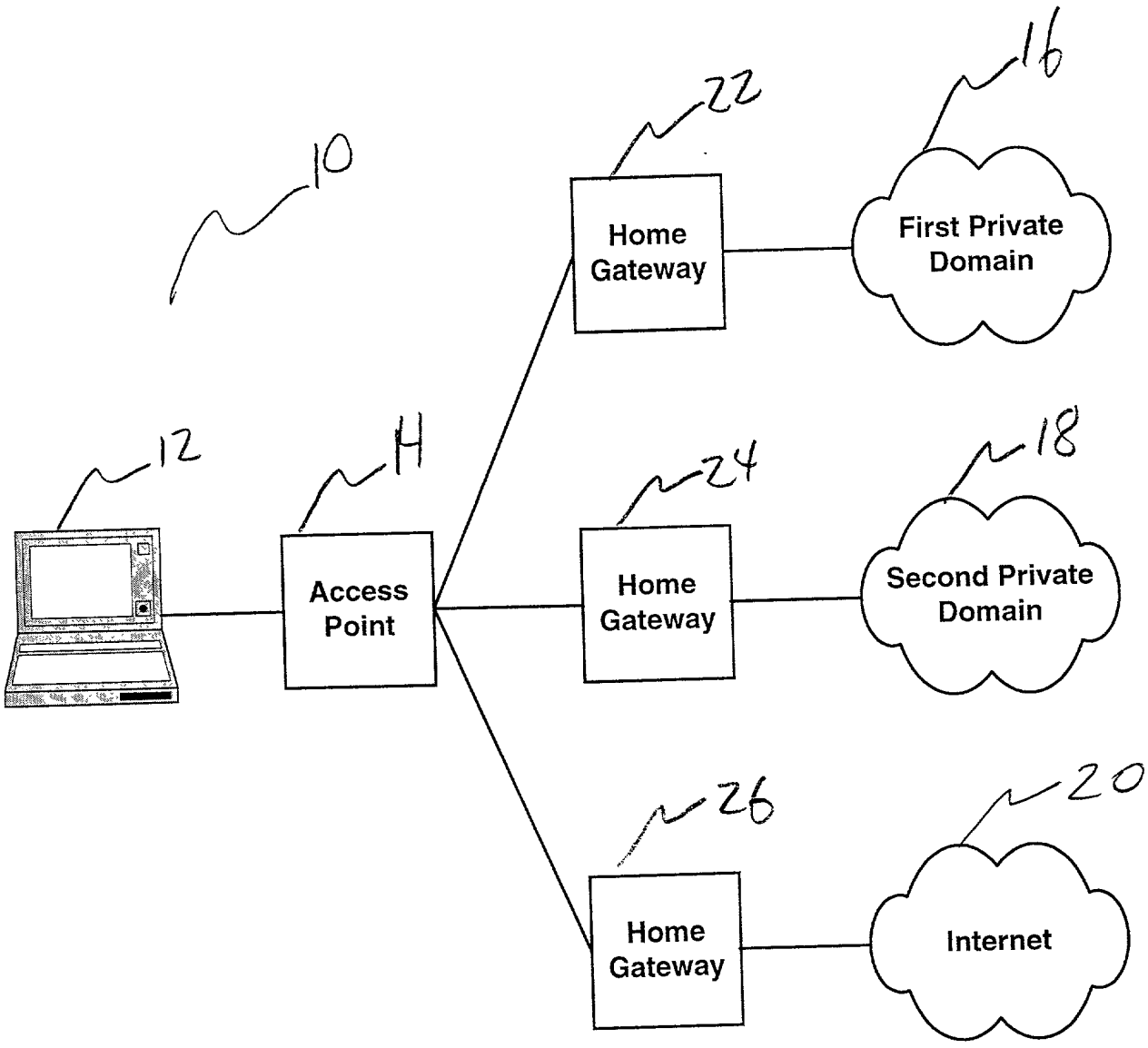

10
12
14
Access Point
22
Home Gateway
16
First Private Domain
24
Home Gateway
18
Second Private Domain
26
Home Gateway
20
Internet

Fig. 1

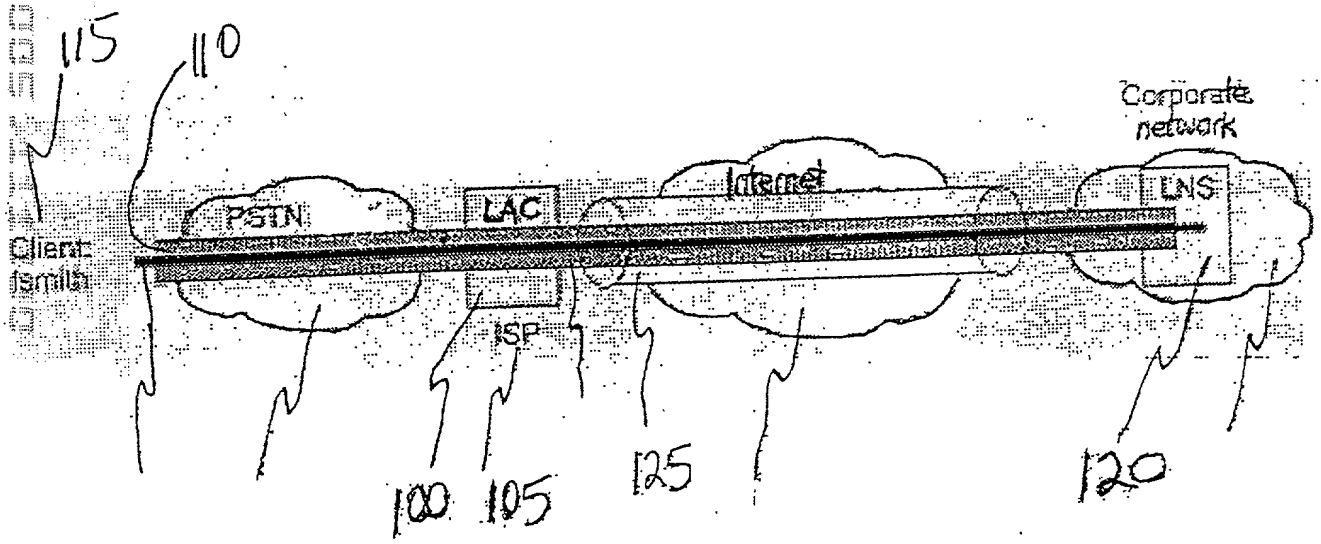

115
110
Corporate network
Internet
PSTN
LAC
LNS
Client: jsmith
ISP
100
105
125
120

Fig. 2

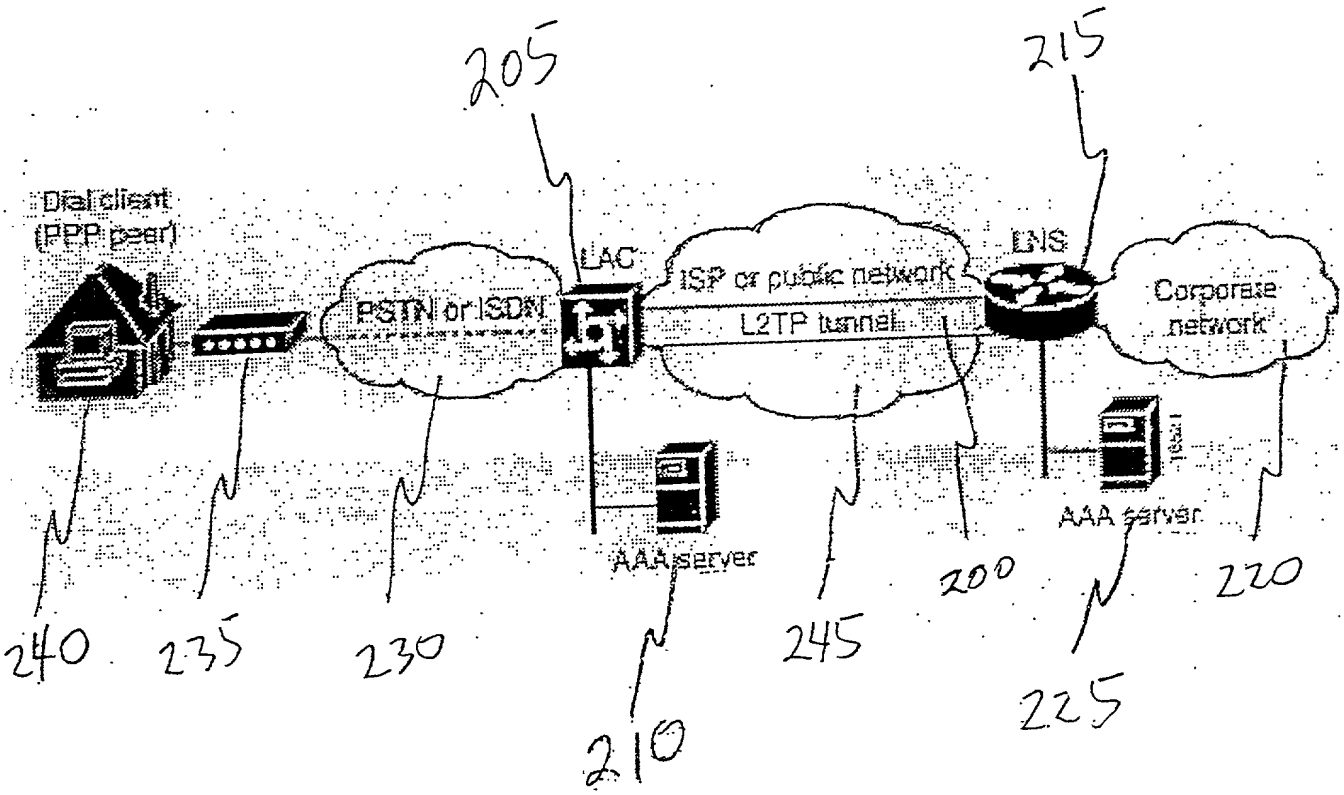

205
215
Dial client
(PPP peer)
LAC
ISP or public network
L2TP tunnel
LNS
PSTN or ISDN
Corporate
network
AAA server
AAA server
240
235
230
210
245
200
225
220

Fig. 3

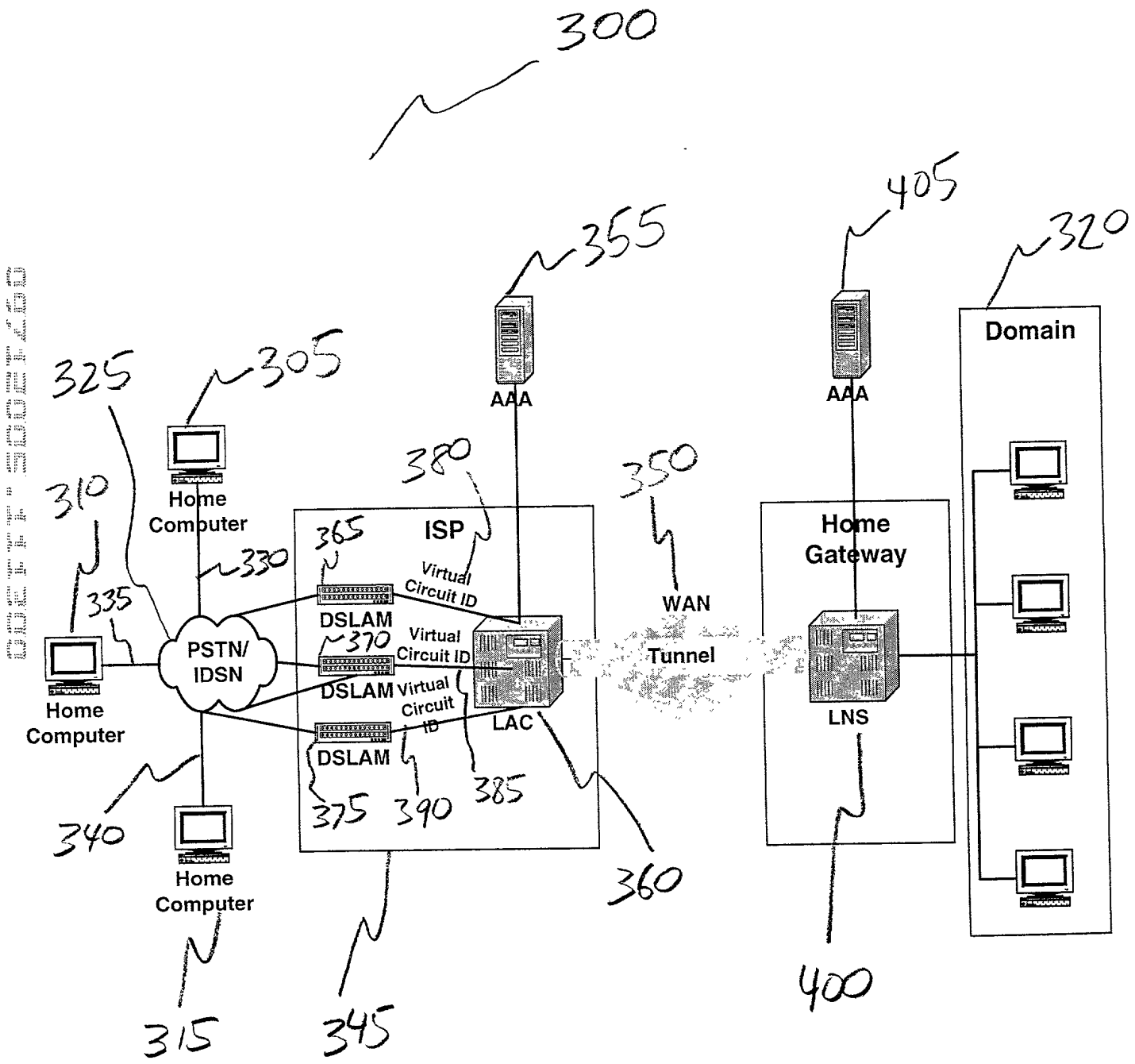

300
355
405
320
AAA
AAA
Domain
325
305
310
Home Computer
380
350
365
ISP
330
Virtual Circuit ID
WAN
Home Gateway
335
DSLAM
370
Virtual Circuit ID
Tunnel
PSTN/ IDSN
Home Computer
DSLAM
Virtual Circuit ID
LAC
LNS
340
DSLAM
375
390
385
360
Home Computer
315
345
400

Fig. 4

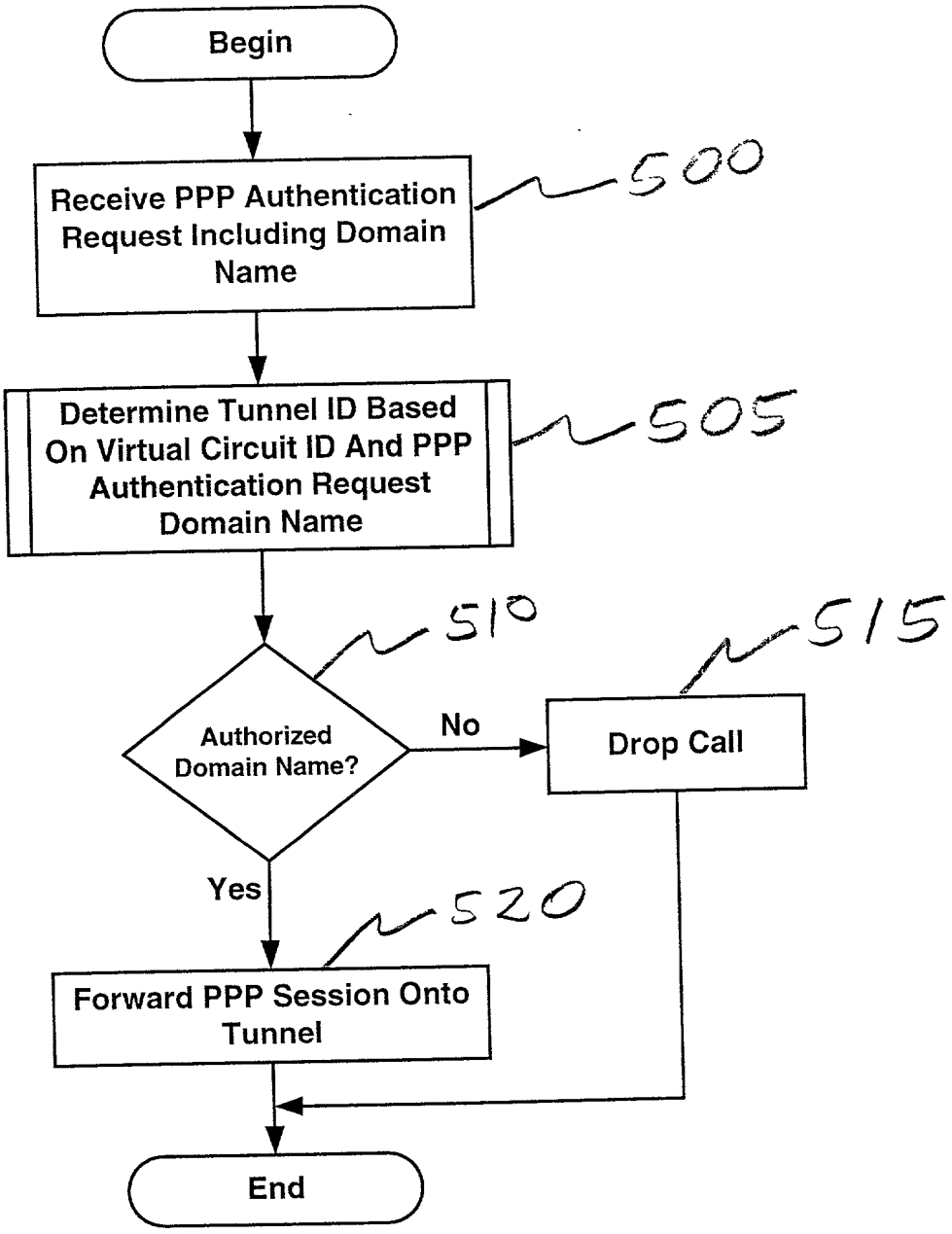

Begin
Receive PPP Authentication Request Including Domain Name
500
Determine Tunnel ID Based On Virtual Circuit ID And PPP Authentication Request Domain Name
505
510
Authorized Domain Name?
No
515
Drop Call
Yes
520
Forward PPP Session Onto Tunnel
End

Fig. 5

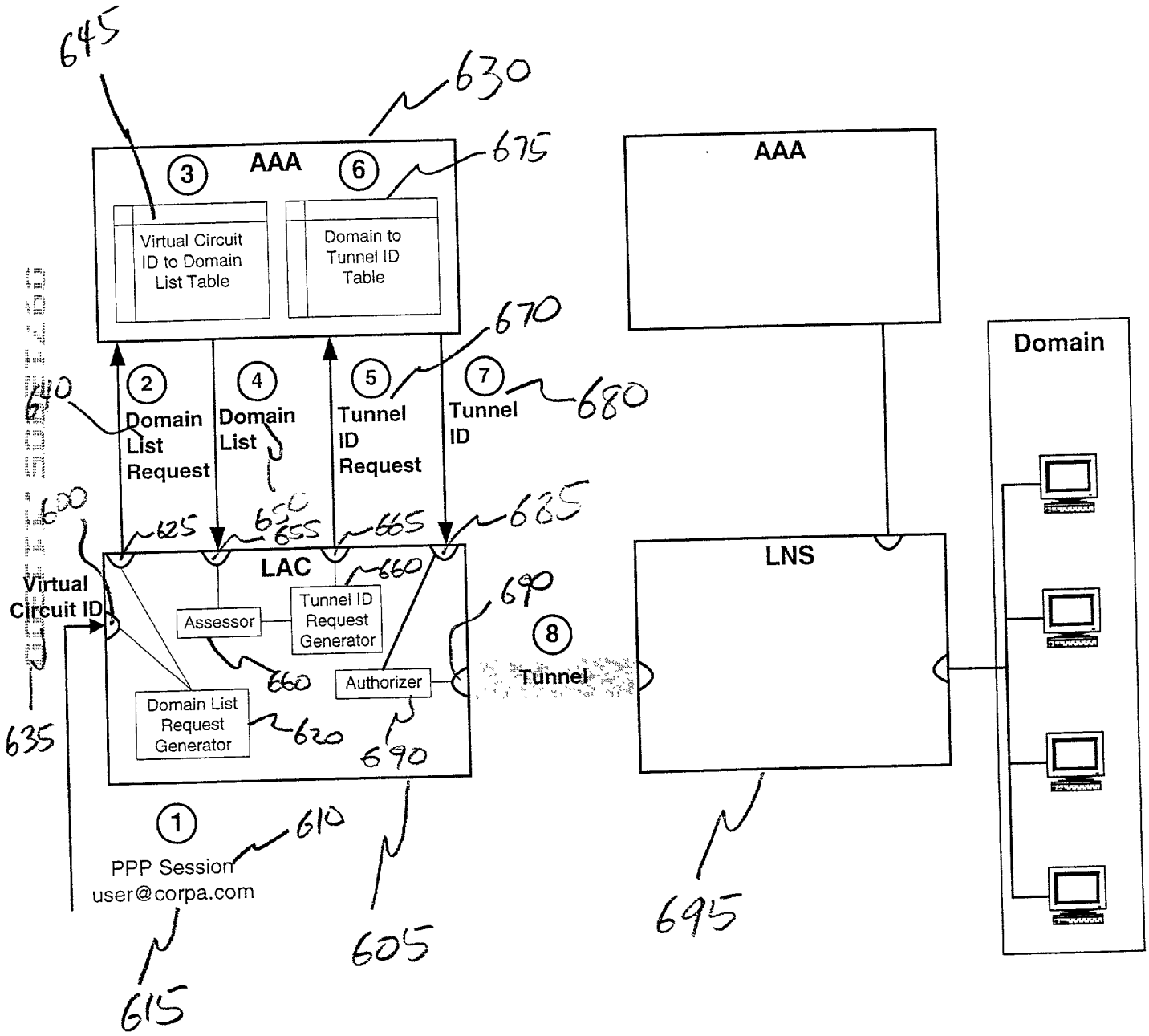

645
630
AAA
3
6
675
Virtual Circuit ID to Domain List Table
Domain to Tunnel ID Table
AAA
Domain
670
2
4
5
7
680
640
Domain List Request
Domain List
Tunnel ID Request
Tunnel ID
600
625
650
655
665
685
LAC
660
690
Virtual Circuit ID
Assessor
Tunnel ID Request Generator
8
Tunnel
LNS
660
Authorizer
Domain List Request Generator
620
635
690
1
610
PPP Session
user@corpa.com
615
605
695

Fig. 6

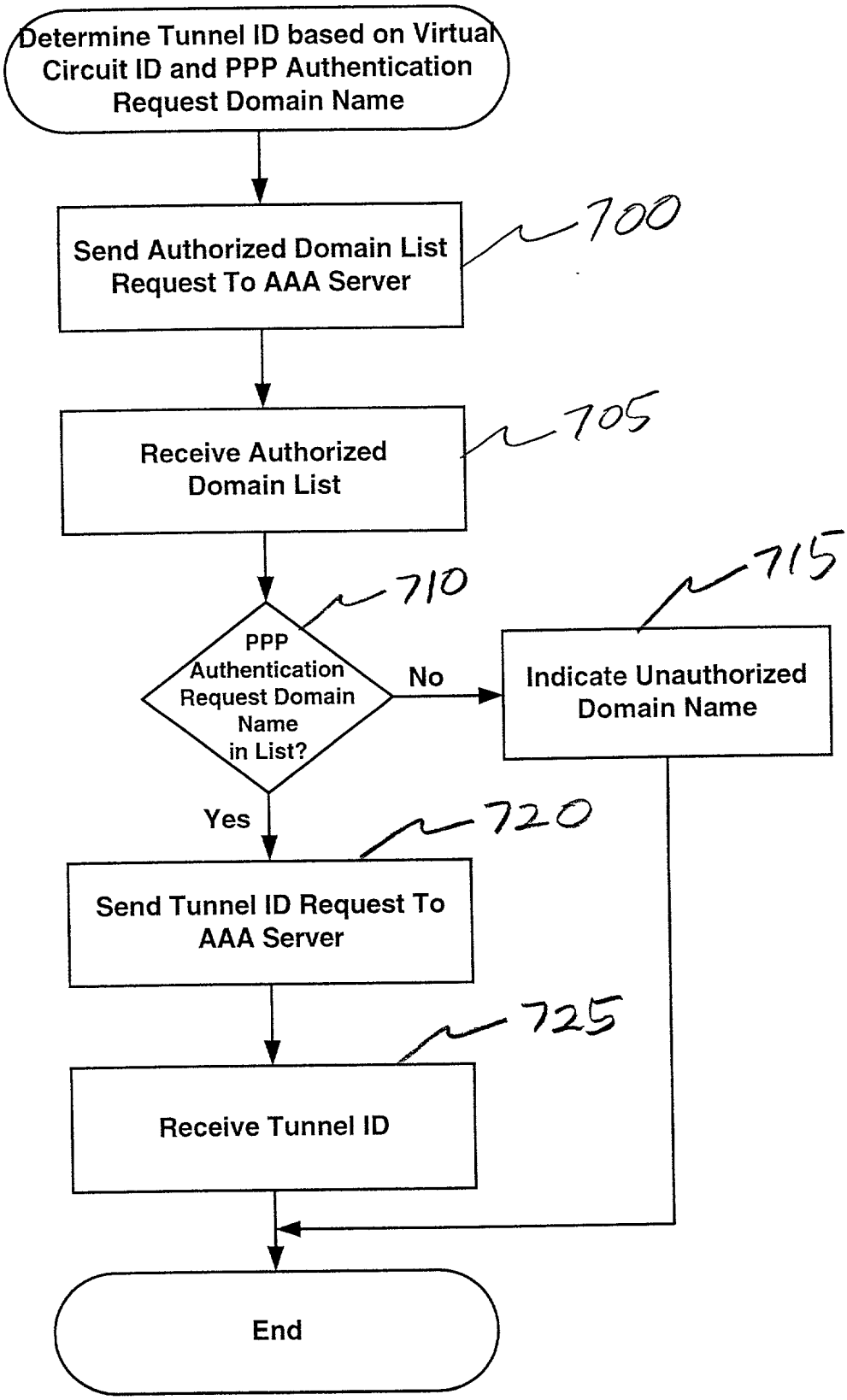

Determine Tunnel ID based on Virtual Circuit ID and PPP Authentication Request Domain Name
Send Authorized Domain List Request To AAA Server
700
Receive Authorized Domain List
705
PPP Authentication Request Domain Name in List?
710
No
Indicate Unauthorized Domain Name
715
Yes
Send Tunnel ID Request To AAA Server
720
Receive Tunnel ID
725
End

Fig. 7

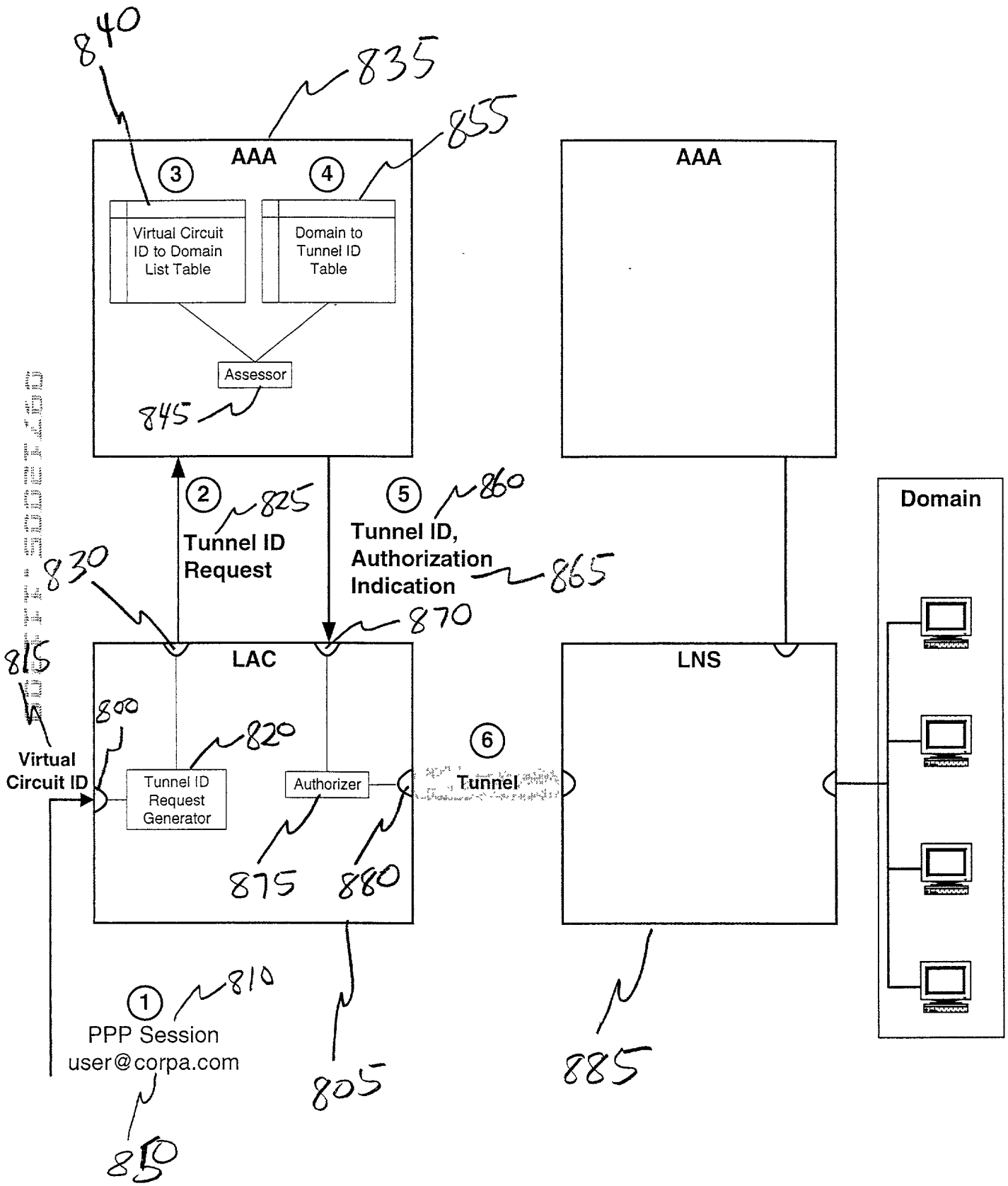

840
835
AAA
855
3
4
Virtual Circuit ID to Domain List Table
Domain to Tunnel ID Table
Assessor
845
AAA
2
825
Tunnel ID Request
5
860
Tunnel ID, Authorization Indication
865
830
870
Domain
815
LAC
LNS
800
820
6
Virtual Circuit ID
Tunnel ID Request Generator
Authorizer
Tunnel
875
880
1
810
PPP Session
user@corpa.com
805
885
850

Fig. 8

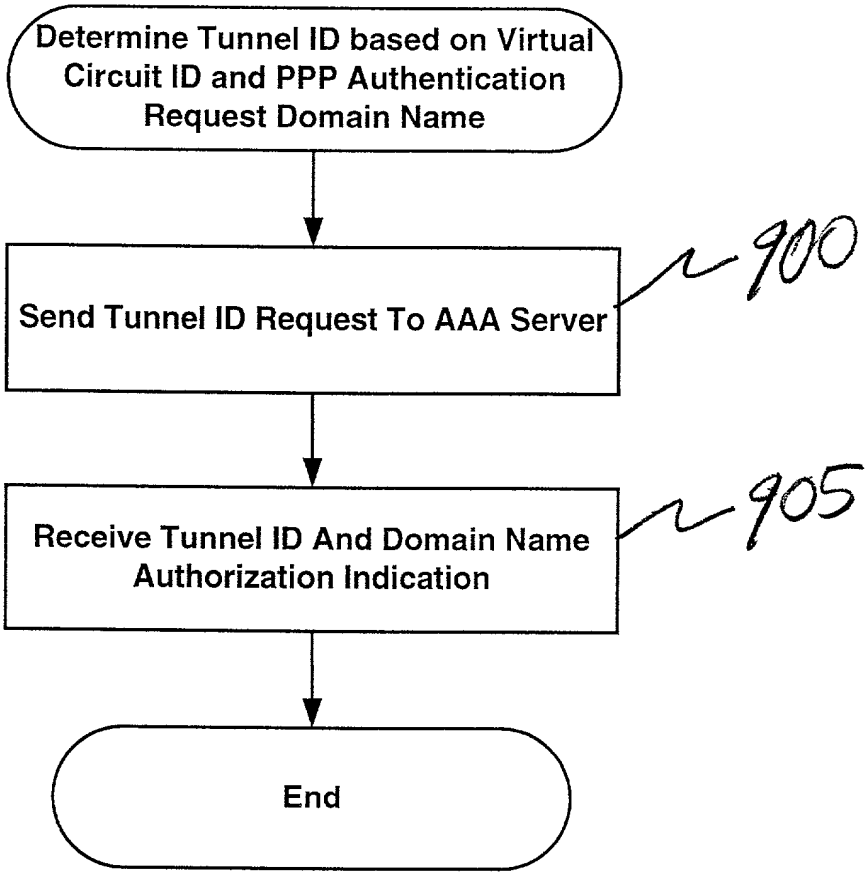

Determine Tunnel ID based on Virtual Circuit ID and PPP Authentication Request Domain Name
Send Tunnel ID Request To AAA Server
900
Receive Tunnel ID And Domain Name Authorization Indication
905
End

Fig. 9

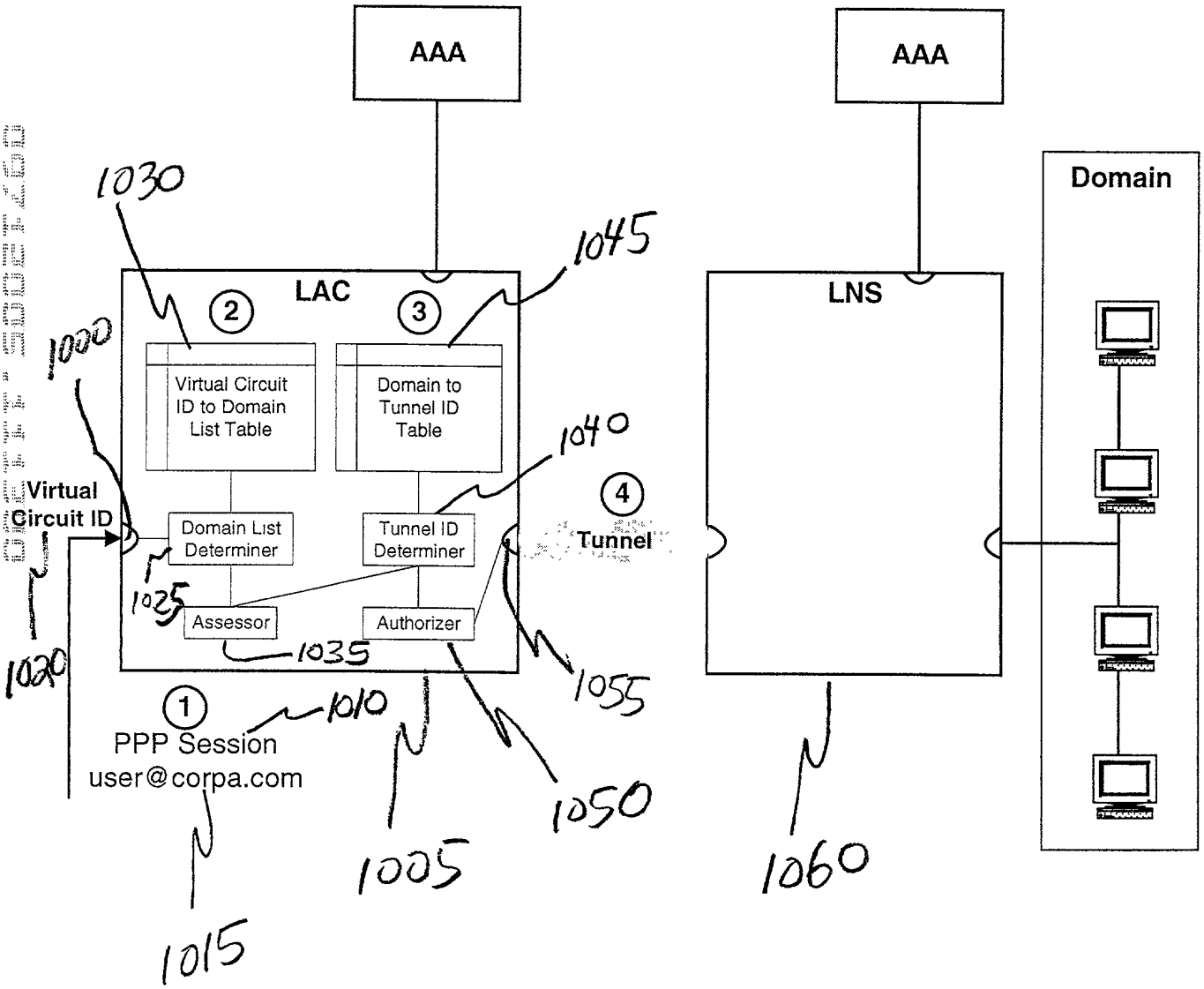

AAA
AAA
Domain
1030
1045
LAC
LNS
2
3
1000
Virtual Circuit ID to Domain List Table
Domain to Tunnel ID Table
1040
4
Virtual Circuit ID
Domain List Determiner
Tunnel ID Determiner
Tunnel
1025
Assessor
Authorizer
1035
1020
1055
1
1010
PPP Session
user@corpa.com
1050
1005
1060
1015

Fig. 10

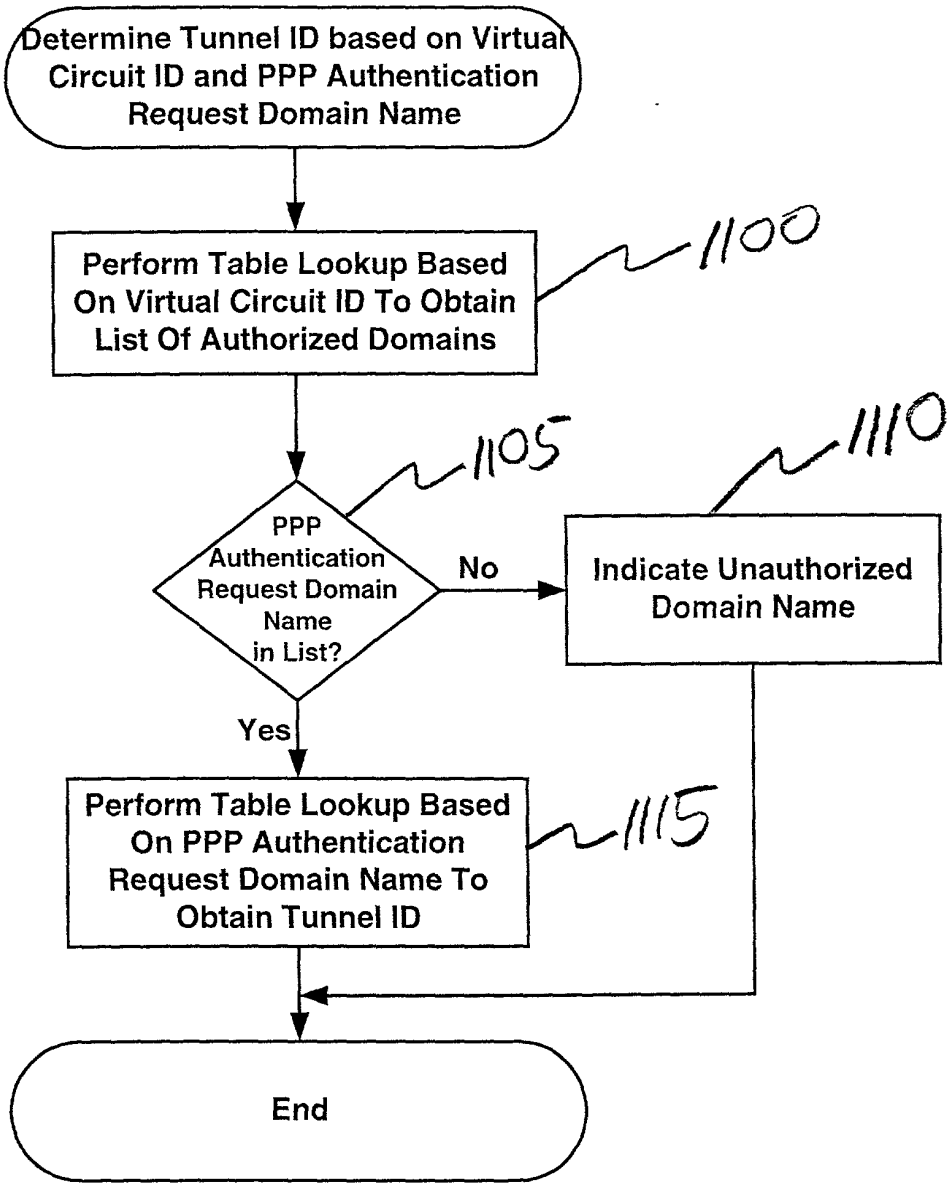
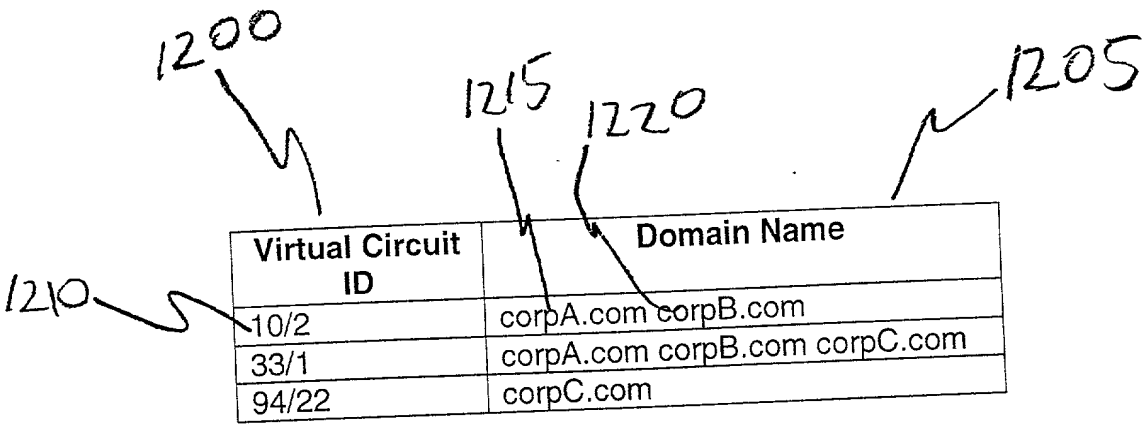
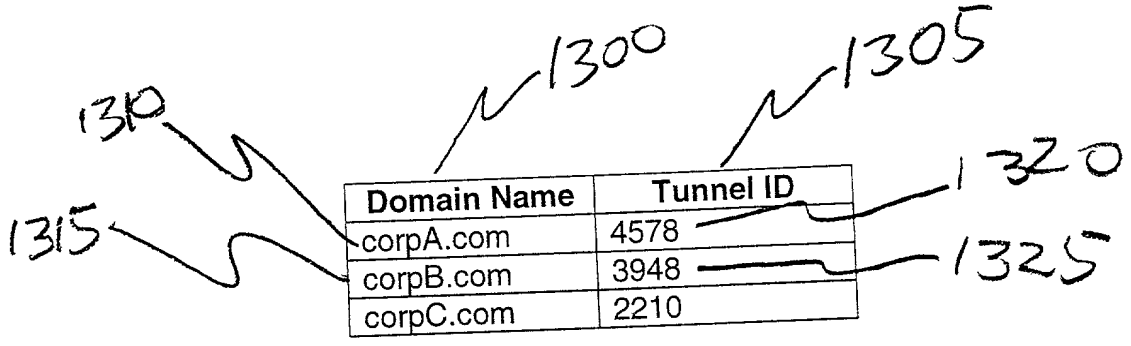

Determine Tunnel ID based on Virtual Circuit ID and PPP Authentication Request Domain Name
Perform Table Lookup Based On Virtual Circuit ID To Obtain List Of Authorized Domains
1100
PPP Authentication Request Domain Name in List?
1105
No
Indicate Unauthorized Domain Name
1110
Yes
Perform Table Lookup Based On PPP Authentication Request Domain Name To Obtain Tunnel ID
1115
End

Fig. 11



Virtual Circuit ID	Domain Name
10/2	corpA.com corpB.com
33/1	corpA.com corpB.com corpC.com
94/22	corpC.com

Fig. 12



Domain Name	Tunnel ID
corpA.com	4578
corpB.com	3948
corpC.com	2210

Fig. 13